

# Stay One Step Ahead of Cyber Attacks

## Raytheon RShield Stops Zero-Day Attacks

Some of the most notorious cyber attacks of late have found their way in through email. Cyber criminals use parasitic stowaway code that can hide on trusted software such as PDFs and then, when it reaches its intended victim goes to work, invisibly, silently, reaping. Terabytes of data and millions of dollars can be gone before an intrusion is detected. Consider the following scenario:

You receive an email from one of your customers with a PDF attachment. You download the document. End of scenario right? Wrong. The email did not come from the trusted customer as you thought, but from an attacker posing as your customer. The PDF has a stowaway parasite—an embedded executable that launches when the PDF is opened. The executable creates a backdoor for cyber criminals giving them access to your hard drive and your organization's network. All this happens in the background—invisible to you.

This exact scenario is how some of the most damaging security breaches have been carried out. These nasty parasites

are not picky about their vehicle, they will leech onto any host they can find: macros, flash files—anything that requires a download.

Companies like Adobe are well aware their software has become targeted hosts and are continually updating to combat the parasites; the problem is cyber criminals continually morph the code to resist the latest patch. Complicating the issue, sophisticated code can defeat incident responders by remaining undetected inside the victim's network, while giving the impression they have been eradicated.

Because cyber criminals will find a way in, and email is a favorite avenue for parasitic code, Raytheon developed RShield. RShield analyzes e-mail and attachments at line speeds by rapidly and seamlessly routing them to virtualized detection farms where they are opened and observed inside a sophisticated, unique and proprietary virtual environment or "sandbox." RShield is able to identify malicious malware even when threat signatures do not exist.

Many malware protection software use sandboxes to detect malicious code and cyber criminals know it, so they include forks and infinite

loops that are inconsequential and benign—successfully hiding their code. Hidden, the malicious attachment gets forwarded and subsequently opened within a hosted environment where it once again looks for signs of a sandbox. With no sandbox around, the malicious code executes and the infection begins. RShield's unique, proprietary sandbox protects against these techniques and is almost impossible to detect; trapping parasitic code and giving it nowhere to hide.

In addition to its sophisticated sandbox, RShield uses behavioral analysis techniques as its primary detection strategy and supplements this with additional heuristics. As protection needs change or grow, as attackers find ways to mutate their attacks, RShield adapts, staying one step ahead of cyber criminals.

---

For further information contact:

**Intelligence and  
Information Systems**  
P.O. Box 660023  
Dallas, Texas  
75266-0023 USA  
iiscommunications@raytheon.com

[www.raytheon.com](http://www.raytheon.com)

*Customer Success Is Our Mission* is a registered trademark of Raytheon Company.

Cleared for International Release. reference #2011-407  
Copyright © 2011 Raytheon Company. All rights reserved.  
CMD011\_00036\_43

**Raytheon**

*Customer Success Is Our Mission*